


PUBLIC LAW 114-113 Guide for Review of Financial Management for CDBG-DR Grantees	
<b>Grantee</b>	Name of Grantee: West Virginia
	Staff Consulted: Lisa Fisher
	Name and Title of Grantee Staff Completing Form: Lisa Fisher, Chief Compliance Officer
	Signature:  Date: 3/22/2017
<b>HUD</b>	HUD Staff Consulted:
	Name and Title of HUD Staff Completing Form:
	Signature: Date:

**Instructions:**

**P.L. 114-113 Certifications:** Each grantee must submit Risk Analysis Documentation to demonstrate in advance of signing a grant agreement that it has in place proficient controls, procedures, and management capacity. This includes demonstrating financial controls, procurement processes, and adequate procedures to prevent any duplication of benefits as defined by section 312 of the Stafford Act. The grantee must also demonstrate that it can effectively manage the funds, ensure timely expenditure of funds, maintain a comprehensive website regarding all disaster recovery activities assisted with these funds, and ensure timely communication of application status to applicants for disaster recovery assistance. Further, the Grantee has established adequate procedures to detect and prevent fraud, waste, and abuse of funds.

In order for Grantees to demonstrate that proficient financial controls are in place, each Grantee must complete this Public Law 114-113 Guide for Review of Financial Management (the Financial Management Guide) as part of completing Part B. Financial Controls of the P.L. 114-113 Risk Analysis documentation and submit the required information to the Grantee's designated HUD representative. A designated HUD representative from Headquarters or the Field Office (FO) must review the Grantee's submission and complete this Financial Management Guide. When HUD CPD Specialists or Financial Analysts are not available, the CPD FO Director will designate an alternate HUD representative for the FO representative. The Headquarter representative will be assigned by the Director of the Disaster Recovery and Special Issues Division.

The Grantee's documentation must be submitted within 30 days of the effective date of the *Federal Register* Notice 5938-N-01 which publishes the Appropriations Act awardees and the grant requirements (the Notice). Failure to submit documentation within 30 days of the effective date of the Notice may result in the cancellation of the award selection. Grantees must submit Risk Analysis documentation in advance of signing a grant agreement in order to demonstrate that grantees can adequately manage and oversee the CDBG-DR award.

This Financial Management Guide is designed to assess the proficiency of a CDBG-DR Grantee's financial controls based on the financial requirements in Subparts D and F of 2 CFR part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. Where the question pertains to a CDBG-DR Grantee, the term Grantee is used.

This Financial Management Guide is a modified exhibit typically used to monitor Grantees following grant execution. To satisfy the requirements for review of financial processes pertaining to the HUD-award, Grantees should consider the processes of existing HUD or other Federal funding awards and refer to documentation of those awards, where applicable. This Financial Management Guide is divided into sections A through J: Financial Management; Internal Controls; Bonds; Payment and Financial Reporting; Cost Sharing or Matching; Program Income; Revision of Budget and Program Plans; Period of Performance; Record Retention and Access; and Audit Requirements. Additionally, in

completing the Financial Management Guide, Grantees must demonstrate that its financial standards are complete and conform to these requirements. The Grantee must identify which sections of its financial standards address each of the questions in the Financial Management Guide and which personnel or unit are responsible for each Financial Management Guide item. As used in this Exhibit, the term "standards" is synonymous with "procedures."

For convenience, certain questions that address financial requirements contain citations to sources that served as the basis for the development of these questions (statute, regulation, NOFA, or grant agreement).

Grantees must identify the type of recipient receiving CDBG-DR grant funds:

	Grantee
State Grantee	<input checked="" type="checkbox"/>
Unit of Local Government (UGLG) Grantee	<input type="checkbox"/>

Please note that all references to "Accounting P&P" in this Guide for Review of Financial Management refer to APPENDIX RFM 1, West Virginia Office of Economic Opportunity's ACCOUNTING AND FINANCIAL POLICY AND PROCEDURES MANUAL.

**PART A. FINANCIAL MANAGEMENT:**

1.

The Grantee must have a system for accounting records to identify adequately the source and application of funds for CDBG-DR-funded activities. The Grantee can facilitate compliance with this requirement if it accounts for a HUD program in a separate accounting fund (e.g., Special Revenue Fund). Note, however, that HUD will not impose specific accounting requirements (such as requiring the Grantee to utilize an accrual basis of accounting).

	Grantee	HUD
a) Does the Grantee have standards to ensure that accounting records contain information on the CDBG-DR grant award, authorizations, obligations, unobligated balances, assets, liabilities, expenditures, program income (as defined by the Notice), and interest?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 4 #3; details begin on page 7 in the Chart of Accounts section; see also "Fund 8746" on pg. 7 under which all information for CDBG - DR award will be captured.</a>		
b) Does the Grantee have standards to maintain adequate source documentation for the information identified in question 1(a)? (To determine compliance, a grantee may select a sample of accounting entries and determine whether they are supported by invoices, contracts, or purchase orders, etc.) [2 CFR 200.302(b)(3)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P Page 4 #3; see Accounts Payable begin on pages 29-33</a>		
c) Does the Grantee have standards established to provide a comparison of expenditures to the budget amounts for the CDBG-DR award? (NOTE: Grantees will usually demonstrate compliance with this requirement by making entries in its accounting records of the amounts budgeted/allocated for activities to be undertaken with the assistance provided under the HUD award which in turn facilitates preparation of financial statements that provide for such comparison.) [2 CFR 200.302(b)(5)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P Page 4 #5; details for Grant Reconciliations begin on page 36</a>		



	Grantee	HUD
d) Does the Grantee have standards requiring it to enter in its accounting records an encumbrance/obligation when contracts are executed, purchase orders issued, etc.? [2 CFR 200.302(b)(3)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P Page 10, Post-Award Procedures #2</a>		
e) Does the Grantee have standards to identify expenditures in its accounting records according to eligible activity classifications specified in the statute, regulations, or grant agreement that clearly identify the use of CDBG-DR funds for eligible activities? [2 CFR 200.302(b)(3)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 26-27, Segregating Unallowable from Allowable Costs #6</a>		
f) Does the Grantee have standards to ensure information on obligations, expenditures, and program income (as defined by the Notice) submitted to HUD in the Disaster Recovery and Grant Reporting System (DRGR), Quarterly Performance Reports (QPR), or other applicable report(s), reconcile with the Grantee's accounting records for time periods reviewed? NOTE: If the Grantee maintains its records on other than an accrual basis, it must be able to support accrual data for its reports on the basis of the documentation on hand. [2 CFR 200.302(b)(2)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 36-37 Grant Reconciliations</a>		

2.

	Grantee	HUD
Does the Grantee have standards to maintain adequate control over all funds, property, and other assets to ensure they are used solely for authorized purposes? See questions below that are related to internal controls. [2 CFR 200.302(b)(4)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 4 #4, page 5-6 Security, and page 8 Control of Chart of Accounts</a>		



**PART B. INTERNAL CONTROLS:**

The Grantee must establish and maintain effective internal controls over the Federal award that provides reasonable assurance that the Grantee is able to manage the Federal award in compliance with this part. These internal controls should be in compliance with guidance in “Standards for Internal Control in the Federal Government” issued by the Comptroller General of the United States (known as the “Green Book”) or the “Internal Control Integrated Framework”, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The definitions of internal control in these documents are intentionally broad. The evaluation of the effectiveness of the Grantee's internal control system likewise must cover a broad range of considerations (e.g., procurement, cost principles.). Further, the audit requirements in 2 CFR part 200, Subpart F include procedures to evaluate the auditee's internal control system. Therefore, the questions below are limited in scope. However, the HUD reviewer should take these considerations into account, together with the questions below, in making an overall assessment of the adequacy of the Grantee's internal controls.

3.

	Grantee	HUD
a) Does the Grantee have standards to perform a self-assessment of its internal control system? [2 CFR 200.303(a)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P - page 45-46, Preparation for Annual Audit, Planning</a>		
b) Does the Grantee have standards to take reasonable measures to safeguard protected personally identifiable information (PII) and other information that HUD or a pass-through entity designates as sensitive, or the Grantee considers sensitive, consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality? (HUD shall verify that the Grantee has a written policy for protecting PII and other safeguard measures.) [2 CFR 200.303(e)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 6 Storage of Sensitive Data; See Appendix RFM-2: Office of Technology Policies, WVOT P0100; WVDOC/OEO is required to follow this policy.</a>		
c) Does the Grantee have the ability to submit an organization chart that sets forth the actual lines of responsibility for the CDBG-DR award?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Describe Basis for Conclusion:</b> <a href="#">See page 3 of Accounting Policies and Procedures; see also Appx. K of the Implementation Plan package.</a>		
d) Does the Grantee have standards to ensure duties and responsibilities are segregated (to the extent practicable) so that no one individual has complete authority over a financial transaction?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No

(For example, the Grantee's procedures preclude one person from issuing purchase orders, receiving merchandise, and approving payment vouchers.)		
--	--	--

**Provide Cross-Reference to Standards:**
[Accounting P&P - page 17 Segregation of Duties](#)
**PART C. BONDS**

4.

	Grantee	HUD
a) Does the Grantee have standards to ensure fidelity bond coverage will be obtained for the responsible officials? [2 CFR 200.304(b)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">West Virginia Code §§ 6-2-1, 6-2-3, 6-2-6. See Appendix RFM-3</a>		

	Grantee	HUD
b) If the answer to 5(a) above is yes, does the Grantee's standards ensure the bond will be from a company holding a certificate of authority as an acceptable surety, as prescribed in 31 CFR Part 223, <i>Surety Companies Doing Business with the United States</i> ? [2 CFR 200.304(c)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<b>Provide Cross-Reference to Standards:</b> <a href="#">West Virginia Code §6-2-2. See Appendix RFM-4</a>		

**PART D. PAYMENT AND FINANCIAL REPORTING:**

5.

	Grantee	HUD
a) If the Grantee is a State, payments under awards that are not governed by a Treasury-State Cash Management Improvement Act (CMIA) agreement, or are not otherwise covered by subpart A of 31 CFR Part 205, must comply with subpart B of that part. If the CDBG-DR award is subject to subpart B, does the Grantee have standards to ensure the timing and amount of funds transfers as close as is administratively feasible to the State's actual cash outlay for direct program costs and the proportionate share of any allowable indirect costs? [2 CFR 200.305(a); 31 CFR 205.33(a)]	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 16-17 Financial Reporting and Cash Drawdowns of Advances</a>		
b) If the State transfers grant funds to subrecipients, does the State have a system to minimize the time elapsing between the receipt of funds from the Federal government and the transfer of funds to the subrecipients? [2 CFR 200.305(a); 31 CFR Part 205, Subpart B]	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A
Describe Basis for Conclusion: <a href="#">Accounting P&amp;P page 37 Cash Flow Management section</a>		

6.

	Grantee	HUD
a) If the Grantee is <b>not a State</b> and transfers grant funds to subrecipients, does the Grantee have standards to ensure the time elapsing is minimized between the receipt of funds from the Federal government and the transfer of funds to the subrecipients? [2 CFR 200.305(b)]	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Yes No N/A	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A
<b>Provide Cross-Reference to Standards:</b>		
b) If the Grantee is <b>not a State</b> , and requests funds in advance, do the Grantee's standards allow the Grantee to minimize the time elapsing between the transfer of funds from the U.S. Treasury and disbursement by the Grantee for direct program or project costs and the proportionate share of any allowable	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> Yes No N/A	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A



indirect costs; and are the advance payments limited to the minimum amounts needed and timed to be in accordance with the actual, immediate cash requirements of the Grantee in carrying out the purpose of the approved project or program? (NOTE: The timing and amount of advance payments must be as close as is administratively feasible to the actual disbursements by the Grantee.)  
[2 CFR 200.305(b)(1)]

**Provide Cross-Reference to Standards:**

7.

	Grantee	HUD
If a Grantee holds cash advances in excess of three business days, including cash advances provided to subrecipients, does the Grantee have standards to provide a sufficient justification? (NOTE: Holding cash advances for a period longer than three business days is not a violation <i>per se</i> ; it may become a preliminary screening measure to determine whether further explanations are required).	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

**Provide Cross-Reference to Standards:**

[Accounting P&P, Page 5 #7 references compliance with 2 CFR Part 200.305](#)

8.

	Grantee	HUD
a) Does the Grantee have standards to disburse funds available from program income (as defined by the Notice), including repayments to a revolving fund), rebates, refunds, contract settlements, audit recoveries, and interest earned on such funds <u>before</u> requesting additional cash payments? [2 CFR 200.305(b)(5)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P Pages 18-20, Program Income</a>		
b) Does the Grantee have standards to ensure advance payments of HUD funds will be deposited and maintained in insured accounts whenever possible? [2 CFR 200.305(b)(7)(ii)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 16, Financial Reporting #6</a>		

c) If the Grantee receives grant advances, does the Grantee have standards to maintain the advance payments in an interest-bearing account <u>or</u> meet one of the following exceptions?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
i. The Grantee receives less than \$120,000 in Federal awards per year.						
ii. The best reasonably available interest-bearing account would not be expected to earn interest in excess of \$500 per year on Federal cash balances.						
iii. The depository would require an average or minimum balance so high that it would not be feasible within the expected Federal and non-Federal cash resources.						
[2 CFR 200.305(b)(8)]						

**Provide Cross-Reference to Standards:**

Exception ii.

9.

	Grantee	HUD
If grant advances will be deposited into an interest-bearing account, does the Grantee have standards for remitting interest income in excess of \$500 annually to the Department of Health and Human Services Payment Management System (PMS) through an electronic medium using either the Automated Clearing House (ACH) network or a Fedwire Funds Service payment? [2 CFR 200.305(b)(9)]	<input type="checkbox"/> Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

**Provide Cross-Reference to Standards:**

N/A per above

**PARTE. COST SHARING OR MATCHING**

11.

	Grantee	HUD
Does the Grantee have standards to ensure contributions meeting cost sharing or matching requirements, including cash and third party in-kind contributions, meet the following criteria:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No
a. Are verifiable from the Grantee's records;		
b. Are not included as contributions for any other Federal award;		
c. Are necessary and reasonable for accomplishment of project or program objectives;		

d. Are allowable under Subpart E—Cost Principles; e. Are not paid by the Federal Government under another Federal award, except as authorized by Federal statute; f. Are provided for in the approved budget when required by HUD; and g. Conform to other provisions of 2 CFR part 200, as applicable? [2 CFR 200.306(b)]		
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 12 Cost Sharing and Matching (In-Kind)</a>		

12.

	Grantee	HUD
a) Does the Grantee have a system to identify unrecovered indirect costs included as a contribution for cost sharing or matching purposes? (NOTE: Unrecovered indirect costs are the difference between the amount charged to the HUD award and the amount which could have been charged to the HUD award under the Grantee's approved negotiated indirect cost rate.) [2 CFR 200.306(c)]	<input checked="" type="checkbox"/> <input type="checkbox"/> Yes No	<input type="checkbox"/> <input type="checkbox"/> Yes No
<b>Describe Basis for Conclusion:</b> <a href="#">Accounting P&amp;P p. 26-29</a>		
b) Does the Grantee have standards to request prior HUD approval of such inclusion? [2 CFR 200.306(c)]	<input checked="" type="checkbox"/> <input type="checkbox"/> Yes No	<input type="checkbox"/> <input type="checkbox"/> Yes No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P p. 26-29</a>		
c) Does the Grantee have standards to identify the non-cash contributions valued in accordance with the requirements at 2 CFR 200.306(d) through (j)? [2 CFR 200.306(d)-(j)]	<input checked="" type="checkbox"/> <input type="checkbox"/> Yes No	<input type="checkbox"/> <input type="checkbox"/> Yes No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P p. 15</a>		



**PART F. PROGRAM INCOME**

12.

	Grantee	HUD
If revenue-generating activities will be undertaken (e.g., rehabilitation loans, economic development loans), does the Grantee have a system to establish revenue accounts in its accounting records to record program income (as defined by the Notice)? [2 CFR 200.302(b)(3)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<b>Describe Basis for Conclusion:</b> <a href="#">Accounting P&amp;P p. 18-20, Program Income</a>		

13.

	Grantee	HUD
a) Does the Grantee have a system to track program income (as defined by the Notice) generated by subrecipients? [2 CFR 200.302(b)(4)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Describe Basis for Conclusion:</b> <a href="#">Accounting P&amp;P p. 18-20, Program Income</a>		
b) Does the Grantee have a system to track program income (as defined by the Notice) retained by the subrecipient for ensuring that such income is reported in a timely and accurate manner? [2 CFR 200.302(b)(2)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Describe Basis for Conclusion:</b> <a href="#">Accounting P&amp;P p. 18-20, Program Income</a>		
c) Upon expiration of any agreements between the Grantee and its subrecipients, does the Grantee have a system to ensure the timely transfer of any funds required to be returned to the Grantee; and/or the timely transfer of outstanding loans or accounts receivable? [2 CFR 200.302(b)(4)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Describe Basis for Conclusion:</b> <a href="#">Accounting P&amp;P p. 18-20, Program Income</a>		

14.

	Grantee	HUD
Does the Grantee have standards to ensure that it will comply with the requirements governing the reporting on receipt and use of program income in the Disaster Recovery Grant Reporting System (DRGR)? [2 CFR 200.302(b)(2)]	<input checked="" type="checkbox"/> <input type="checkbox"/> Yes No	<input type="checkbox"/> <input type="checkbox"/> Yes No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Acc. P&amp;P - page 37 Federal Award Reporting and pages 18-20, Program Income</a>		

**PART G. REVISION OF BUDGET AND PROGRAM PLANS**

15.

	Grantee	HUD
a) Does the Grantee have standards to ensure that any changes made to the approved project's budget, scope, or objectives will be identified to HUD?	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P p. 45 Budget Modifications</a>		

	Grantee	HUD
b) Does the Grantee have standards to require HUD approval before making any of the following changes to a non-construction award?	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Yes No N/A
i. Change in the scope or the objective of the project or program (even if there is no associated budget revision requiring prior written approval).		
ii. Change in a key person specified in the application or the Federal award.		
iii. The disengagement from the project for more than three months, or a 25 percent reduction in time devoted to the project, by the approved project director or principal investigator.		
iv. The inclusion, unless waived by HUD, of costs that require prior approval in accordance with Subpart E—Cost Principles of 2 CFR part 200, or 45 CFR part 75 Appendix IX, <i>Principles for Determining Costs Applicable to Research and Development under Awards and Contracts with Hospitals</i> , or 48 CFR part 31, <i>Contract Cost Principles and Procedures</i> , as applicable.		
v. The transfer of funds budgeted for participant support costs as defined in §200.75, <i>Participant support costs</i> ,		

vi. to other categories of expense. Unless described in the application and funded in the approved Federal awards, the subawarding, transferring or contracting out of any work under a Federal award, including fixed amount subawards as described in §200.332, <i>Fixed amount subawards</i> (this provision does not apply to the acquisition of supplies, material, equipment or general support services). vii. Changes in the approved cost sharing or matching provided by the Grantee. viii. The need arises for additional Federal funds to complete the project. [2 CFR 200.308(c)(1)]		
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P Page 44 Budget and Program Revisions</a>		

16.

	Grantee			HUD		
Does the Grantee have standards to require HUD approval before making any of the following budget revisions whenever (a), (b), or (c) below applies to a construction award?  a. The revision results from changes in the scope or the objective of the project or program. b. The need arises for additional Federal funds to complete the project. c. A revision is desired which involves specific costs for which prior written approval requirements may be imposed consistent with applicable OMB cost principles listed in 2 CFR part 200, Subpart E—Cost Principles. [2 CFR 200.308(g)]	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Yes	No	N/A	Yes	No	N/A
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P p. 45 Budget Modifications</a>						

**PARTH. PERIOD OF PERFORMANCE**

17.

	Grantee		HUD	
Does the Grantee have standards to ensure it will charge to the HUD award only allowable costs (except as described in §200.461, <i>Publication and printing costs</i> ) incurred during the period of performance and authorized pre-award costs?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Yes	No	Yes	No



[2 CFR 200.309]

**Provide Cross-Reference to Standards:**  
[Accounting P&P page 26-29 Charging of Costs to Federal Awards](#)

## PART I. RECORD RETENTION AND ACCESS

18.

Grantee	HUD	Grantee
Does the Grantee have standards to comply with applicable record retention and access requirements? [24 CFR 570.502; or 24 CFR 570.490]	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 49 Record Retention</a>		

## PART J. AUDIT REQUIREMENTS

Instructions: A Grantee that expends \$750,000 or more during the Grantee's fiscal year in Federal awards must have a single or program-specific audit conducted for that year in accordance with the provisions of 2 CFR part 200, Subpart F, *Audit Requirements*. Grantees that provide Federal awards to subrecipients are referred to as "pass-through entities." A subrecipient must also have a single or program-specific audit if it meets the \$750,000 expenditure threshold. Pass-through entities are required by 2 CFR 200.331 to ensure compliance with Subpart F. A Grantee that expends less than \$750,000 in Federal awards during the entity's fiscal year is exempt from audit requirements for that year, except as noted in 2 CFR 200.503. This section of questions is designed to assist the HUD reviewer in determining whether the Grantee is able to comply with the required elements of an audits management system.

19.

	Grantee	HUD
Does the Grantee have standards to meet the annual expenditure threshold (\$750,000) for having a single or program-specific audit conducted? If "no," skip questions 22 through 27.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P pages 45-48, Annual Audit. The Financial Accounting and Reporting Section (FARS) within the State Auditor's Office ensures the performance of a single audit each fiscal year.</a>		

20.

	Grantee	HUD
a) Does the Grantee have standards to procure or arrange for the audit services in accordance with the procurement standards at 2 CFR 200.317 – 200.326? [2 CFR 200.508(a) and 2 CFR 200.509]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">State Auditor procures audit services under West Virginia Purchasing Division Procedures Handbook Section 3.7.1.2. See Appendix RFP-5</a>		
b) Does the Grantee have standards to request for proposal audit services that clearly state the objectives and scope of the audit? NOTE: the Grantee requests a copy of the audit organization's peer review report which the auditor is required to provide under Generally Accepted Government Auditing Standards (GAGAS)? [2 CFR 200.509(a)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">State Auditor procures audit services under West Virginia Purchasing Division Procedures Handbook Section 6. See Appendix RFP-5</a>		
c) Does the Grantee have standards to apply the factors, to be considered in evaluating the proposal for audit services which include the responsiveness to the request for proposal, relevant experience, availability of staff with professional qualifications and technical abilities, the results of peer and external quality control reviews, and price? [2 CFR 200.509(a)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">State Auditor procures audit services under West Virginia Purchasing Division Procedures Handbook Section 6.2.4. See Appendix RFM-5</a>		
d) Does the Grantee have standards to make positive efforts to utilize small businesses, minority-owned firms, and women's business enterprises, in procuring audit services as stated in §200.321, <i>Contracting with small and minority businesses, women's business enterprises, and labor surplus area firms</i> ? [2 CFR 200.509(a)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">See West Virginia Purchasing Division Procedures Handbook, Sections 4.4 and 6.3.2. See Appendix RFM-5</a>		

21.

	Grantee	HUD
Does the Grantee have standards for the auditee prepare financial statements, including the schedule of expenditures of Federal awards, required by 2 CFR 200.510? [2 CFR 200.508(b)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">West Virginia State Auditor includes this requirement each year in the scope of services for its external auditor.</a>		

22.

	Grantee	HUD
Does the Grantee have standards to promptly follow up and take corrective action on audit findings, including preparation of a summary schedule of prior audit findings and a corrective action plan in accordance with 2 CFR 200.511(b) and 2 CFR 200.511(c), respectively? [2 CFR 200.303(d) and 2 CFR 200.508(c)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P page 45-47</a>		

23.

	Grantee	HUD
Does the Grantee have a system to electronically submit to the Federal Audit Clearinghouse the data collection form described in 2 CFR 200.512(b) and reporting package described in 2 CFR 200.512(c) within the earlier of 30 calendar days after receipt of the auditor's report(s), or nine months after the end of the audit period? [2 CFR 200.512(a) and (d)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Describe Basis for Conclusion:</b> <a href="#">Accounting P&amp;P page 45, Role of the Independent Auditor</a>		

24.

	Grantee	HUD
a) Does the Grantee have standards to inform subrecipients of the 2 CFR part 200, Subpart F audit requirements at the time of the subaward? [2 CFR 200.331(a)(2)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No



<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P pages 23-25, Monitoring of Subrecipients</a>			
b) Does the Grantee have standards to verify that every subrecipient is audited, as required by Subpart F, when it is expected that the subrecipient's Federal awards expended during the respective fiscal year equaled or exceeded the \$750,000 expenditure threshold? [2 CFR 200.331(f)]	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P p. 24 #9</a>			
c) Does the Grantee have standards to ensure that the subrecipients take timely and appropriate action on all deficiencies pertaining to HUD awards it provided to subrecipients that were detected through audits, on-site reviews and other means? [2 CFR 200.331(d)(2)]	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P Page 24-25 #10f and 12</a>			
d) Does the Grantee have standards to issue a management decision for audit findings that relate to HUD awards that it makes to subrecipients? [2 CFR 200.331(d)(3)]	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P p. 24 #9, Monitoring of Subrecipients</a>			

25.

	Grantee	HUD
Does the Grantee have standards to ensure that the HUD award is charged no more than a reasonably proportionate share of the costs of audits required by, and performed in accordance with 2 CFR part 200, Subpart F? [2 CFR 200.425(a)]	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">Accounting P&amp;P p.24 #9, Monitoring of Subrecipients</a>		

26.

When a auditee expends Federal awards under only one Federal program and the Federal program's statutes, regulations, or the terms and conditions of the Federal award do not require a financial statement audit of the auditee, the auditee may elect to have a program-specific audit conducted in accordance with §200.507, *Program-specific audits*. When a program-specific audit is elected for a HUD program, the auditee and auditor must have basically the same responsibilities for the Federal program as they would have for an audit of a major program in a single audit. Answer the following questions only if the Grantee has elected to have a previous program-specific audit performed.

	Grantee	HUD
a) Does the Grantee have standards to ensure the auditee prepared the financial statement(s) for the HUD program that includes, at a minimum, a schedule of expenditures of Federal awards for the program and notes that describe the significant accounting policies used in preparing the schedule, a summary schedule of prior audit findings consistent with the requirements of 2 CFR 200.511(b), and a corrective action plan consistent with the requirements of 2 CFR 200.511(c)? [2 CFR 200.507(b)]	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Provide Cross-Reference to Standards:</b> <a href="#">West Virginia does not anticipate conducting a program specific audit.</a>		
b) Does the Grantee have a system to electronically submit to the Federal Audit Clearinghouse the reporting package required by 2 CFR 200.507(c)(3) and the data collection form prepared in accordance with 2 CFR 200.512(b) within the earlier of 30 calendar days after receipt of the auditor's report(s), or nine months after the end of the audit period? [2 CFR 200.507(c)]	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
<b>Describe Basis for Conclusion:</b> <a href="#">West Virginia does not anticipate conducting a program specific audit.</a>		



State of West Virginia Office of Technology Policy:  
**Information Security**  
*Issued by the CTO*

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 1 of 14

---

## 1.0 PURPOSE

This policy, issued by the West Virginia Office of Technology (WVOT) establishes objectives and responsibilities for all West Virginia state government agencies, employees, vendors, and business associates, specifically the Executive, regarding information security and the protection of information resources. The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided information technology (IT) resources and is not necessarily all-inclusive. IT resources may include anything with a processor, communications capability, or data storage. (See Appendix A, "Technology Usage Practices" for a list of examples.)

---

## 2.0 SCOPE

This document applies to all employees with access to information and the systems that store, access, or process that information. Questions about specific security-related uses which are not detailed in this policy should be directed to a supervisor or manager.

---

## 3.0 POLICY

- 3.1 All IT assets, including hardware, software, and data, are owned by the State, unless accepted by contractual agreement.
- 3.2 Users are required to comply with legal protection granted to programs and data by copyright and license. No unauthorized software will be installed on State systems. The WVOT or its equivalent will authorize all software installation.
- 3.3 Users will utilize, maintain, disclose, and dispose of all information resources, regardless of medium, according to law, regulation, and/or policy.
- 3.4 **Employees must have no expectation of privacy while using State-provided information resources (e.g. cell phones, Internet, etc.).**
- 3.5 The State reserves the right to filter Internet site availability, and monitor and review employee use as required for legal, audit, or legitimate authorized State operational or management purposes.
- 3.6 Agencies are required to have employees sign a policy Statement of Acknowledgement, which will recognize that the employee has read the document and will periodically review the WVOT policy and procedure for updates. Employees may be denied the use of information resources by refusing to sign.
- 3.7 All employees must adhere to rules regarding unacceptable uses of IT resources. (For a detailed list of unacceptable uses, see appendix A, "Technology Usage Practices")



# Policy: Information Security

## State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 2 of 14

- 3.7.1 Employees must not download, attach, change, distribute, or install any software or inappropriate files, including streaming content, for non-business functions (e.g. downloading MP3 files and/or broadcast audio or video files).
- 3.7.2 Employees must not intentionally introduce a virus into a State-provided computer, or withhold information necessary for effective virus control procedures.
- 3.7.3 Employees must not send or share confidential information for unauthorized purposes.
- 3.7.4 Employees must not attach or use devices on the State network that are not owned by the State or authorized by the WVOT.
- 3.7.5 Employees must not redirect confidential or privileged State data to a non-State owned computing device or PDA without proper authorization.
- 3.7.6 Employees must not use unauthorized peer-to-peer networking or peer-to-peer file sharing.
- 3.7.7 Employees must NEVER execute programs or open e-mail attachments that: (1) have not been requested; or (2) come from an unknown source. If in doubt and lacking assurance from the sender, employees should contact the WVOT Service Desk for assistance.
- 3.7.8 Employees must never attempt to disable, defeat, or circumvent any security firewalls, proxies, web filtering programs, or other security controls.
- 3.7.9 Employees must not use IT resources to promote harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability.
- 3.8 The WVOT, working with designated individuals, will develop procedures to protect information resources from accidental, unauthorized, or malicious access, disclosure, modification, or destruction.
- 3.9 Users must report any observation of attempted security or privacy violations to [incident@wv.gov](mailto:incident@wv.gov).
  - 3.9.1 A Security Incident is any event that involves misuse of computing resources or is disruptive to normal system or data processing operations. Examples include, but are not limited to the following:
    - Lost or stolen computers or other portable devices;
    - Lost or stolen media that contains sensitive data;

# Policy: Information Security

## State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 3 of 14

- Rampant computer virus infections within the State network;
- Loss of system or network functionality;
- A disaster scenario or act of terrorism;
- A prolonged power outage;
- A compromised (hacked) computer or server;
- A defaced Web page; and
- An information security policy violation.

3.10 Users should immediately report all information security incidents to [incident@wv.gov](mailto:incident@wv.gov). Users must provide the following information, to the extent possible:

3.10.1 Point of contact (name, phone, e-mail);

3.10.2 Characteristics of incident;

3.10.3 Date and time incident was detected;

3.10.4 Extent of impact;

3.10.5 Nature of incident, if known (ex: unauthorized access, system breach or malfunction, data loss or exposure, defacement, other); and

3.10.6 Any actions taken in response to the incident.

3.11 Confidential, private, personally identifiable information (PII), Federal Tax Information (FTI), or other sensitive data (i.e. credit card numbers, calling card numbers, logon passwords, health information, or other protected information), must be encrypted or disassociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.

3.12 Employees must immediately contact [incident@wv.gov](mailto:incident@wv.gov) upon receiving or obtaining confidential information to which the employee is not entitled (Note: the owner or sender of such information must also be notified) or becoming aware of any inappropriate use of State-provided IT resource.

3.13 Employees will contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.

3.14 Access controls must be consistent with all state and federal laws and statutes, and will be implemented in accordance with this policy.



## Policy: Information Security

### State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 4 of 14

- 3.15 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.
  - 3.15.1 All passwords are confidential and **must not** be shared under any circumstances.
  - 3.15.2 Employees are expected to use strong passwords, which must conform to established standards and will be changed at intervals designated by the CTO.
- 3.16 All access to computing resources will be granted on a need-to-use basis.
- 3.17 Individual users will be assigned unique userids.
- 3.18 Each employee must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.
- 3.19 The WVOT will provision network user accounts by adding, modifying, and deleting user access for customer agencies. Each agency will appoint a designated approval authority, who will authorize all access modifications for that agency.
  - 3.19.1 When an employee is terminated, the agency's designated approval authority must contact WVOT immediately to disable all access, unless otherwise approved in writing by appropriate management.
  - 3.19.2 When an employee transfers, WVOT will modify all access to accommodate new user roles and responsibilities according to instructions from the agency's designated approval authority.
- 3.20 All Executive Branch employees will be required to complete mandatory online information security awareness or refresher training annually. New employees will be required to complete mandatory online training within the first week of employment as part of job orientation.
- 3.21 The authorized head of each agency (agency head) must assure that all employees sign a confidentiality agreement upon hire and annually thereafter. This confirms that the employee has read, fully comprehends, and will abide by State policies and procedures regarding privacy and information security.
- 3.22 The agency head must assure that all employees, and others who access computer systems, will receive sufficient training in policies and procedures, security requirements, correct use of information resources, and other administrative controls.



# Policy: Information Security

## State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 5 of 14

3.23 The agency head must assure that all employees receive an appropriate background check (where applicable) consistent with legislative rule and West Virginia Division of Personnel policy.

### 3.24 Data/Information Assets

3.24.1 Information resources are designated for authorized purposes. The State has a right and a duty to review questionable employee activity. Only minimal personal use of State-provided IT resources is permitted (e.g. 10-15 minutes during break and/or lunch periods). This must not include any unauthorized uses (see appendix A) and must not interfere with the legitimate business of the State.

3.24.2 All information assets must be accounted for and have an assigned owner. Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented.

3.24.3 Each owner or custodian of information will determine and document classification based on the circumstances and the nature of the information, according to a classification scheme common to all State agencies. Classification should consider legal protections, privacy, sensitivity, and criticality to the functions of the business. (For more information see WVOT-PO1006 – “Data Classification.”)

3.24.4 The owner or custodian will determine and document the data classification, and the agency Information Security Administrator (ISA) will ensure the protective guidelines that apply for each level of information. They include, but may not be limited to the following:

- Access
- Use Within <Agency>
- Disclosure Outside <Agency>
- Electronic Distribution
- Disposal/Destruction

3.24.5 If at any time equipment or media changes ownership or is ready for disposal, the user must alert the responsible technical staff to the potential presence of any confidential and/or sensitive data on said equipment or media.

### 3.25 Physical and Environmental Security

3.25.1 Information resource facilities will be physically secured by measures appropriate to their critical importance.

# Policy: Information Security

## State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 6 of 14

- 3.25.2 Security vulnerabilities will be determined, and controls will be established, to detect and respond to threats to facilities and physical resources.
- 3.25.3 Employees must guard against access to files and take precautions to protect IT devices when away from the workstation. This includes but may not be limited to the following:
  - Logging off computer;
  - Locking computer; and/or
  - Locking file cabinets and drawers.
- 3.25.4 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.
- 3.25.5 Equipment will be secured and protected from physical and environmental damage.
- 3.25.6 Equipment used outside State premises will be given an equal or greater degree of security protection as that of on-site information resource equipment.

### 3.26 Information Security Administrators

- 3.26.1 The departmental head must assign the role of Information Security Administrator (ISA). The ISA must perform, contract, or delegate the necessary functions and responsibilities of the position as defined in this policy and the Governor's Executive Information Security Team (GEIST) charter. If necessary, the ISA may delegate duties to one or more individuals (ex: ISL's) whose main function will be to assist in the protection of information resources within their agency.
- 3.26.2 The ISA will ensure that a risk management program will be implemented and documented, and that a risk analysis will be conducted periodically.
- 3.26.3 The ISA will oversee and ensure that cost effective contingency response and recovery plans will be maintained, providing for prompt and effective restoration of critical business functions in the event of any disruptive incident.
  - 3.26.3.1 Procedures, guidelines, and mechanisms utilized during an information\_security incident, along with the roles and responsibilities of the incident management teams, must be established, documented, and periodically reviewed. This may include testing to make sure that all plans remain current, viable, and comprehensive.

# Policy: Information Security

## State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 7 of 14

- 3.26.3.2      Testing will be performed at intervals designated within CTO standards.

---

### 4.0 RELEVANT DOCUMENTS/MATERIAL

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO),  
[www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx](http://www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx)

---

### 5.0 ENFORCEMENT & AUTHORITY

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the **West Virginia Division of Personnel**. Please review the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

---

### 6.0 DEFINITIONS

- 6.1      Access— The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.
- 6.2      Access Controls – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.
- 6.3      Authentication – The process of verifying the identity of a user.
- 6.4      Chief Information Security Officer (CISO) – Person designated by the CTO to oversee information security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.
- 6.5      Chief Technology Officer (CTO) – The person responsible for the State's information resources.



# Policy: Information Security

## State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 8 of 14

- 6.6 Confidential Data – Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.
- 6.7 Contractor – Anyone who has a contract with the State or one of its entities.
- 6.8 Custodian of Information – The person or unit assigned to supply services associated with the data.
- 6.9 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of information technology and security policy, the term “employee” shall include the following: contractors, subcontractors, contractors’ employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.
- 6.10 Information Assets – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.
- 6.11 Information Resources – All information assets, in all known formats.
- 6.12 Information Security – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.
- 6.13 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency’s compliance with State information security policies and procedures. The ISA is the agency’s internal and external point of contact for all information security matters.
- 6.14 Information Security Incident – An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.
- 6.15 Information Security Liaison (ISL) - Employees assigned by the ISA to assist in the protection of information resources.
- 6.16 Information Technology (IT) – The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.
- 6.17 Medium – Any repository, including paper, used to record, maintain, or install information or data.
- 6.18 Owner of Information – The person(s) ultimately responsible for an application and its data viability.

# Policy: Information Security

## State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 9 of 14

- 6.19 Password – A string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.
- 6.20 Personally Identifiable Information (PII) – Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.
- 6.21 Privacy Officer - The official responsible for facilitating the Executive Branch's integration of privacy principles, legal requirements, and privacy standards into department policies, procedures, and practices.
- 6.22 Procedure – A set of instructions or process steps prescribed in sufficient detail in order to understand how to meet a policy requirement. Procedures should document roles, methods, options, and examples necessary for a reader to understand how to comply with a policy.
- 6.23 Risk Analysis – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.
- 6.24 Security Contact – These individuals include the ISA or the ISL.
- 6.25 Threat – Includes any person, condition, or circumstance that endangers the security of information or information systems in the context of information security.
- 6.26 User – A person authorized to access an information resource.
- 6.27 User id – A unique “name” by which each user is identified to a computer system.
- 6.28 West Virginia Division of Personnel – A division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq.*, which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.
- 6.29 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.*, which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

---

## 7.0 Change Log History

- January 28, 2015 – Added Change Log History; Split Section 4.5 into two sections, 4.5 and 4.6, respectively. Modified 4.6 to begin “Agencies are required to have employees sign....”

## Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 9/1/2016

Page 10 of 14

- 9/1/2016 - Policy Reviewed. No edits made.



# Appendix A: Technology Usage Practices

## Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 07/01/2015

Page 11 of 14

---

### Acceptable/Unacceptable Use of State-Provided Technology:

The information contained within this Appendix applies to the State of West Virginia Information Security policy.

#### Relevant Technologies Include, but may not be limited to the following:

- a. Personal computers
- b. Personal Digital Assistants (PDA)
- c. Fax or copy machines with memory or hard drives
- d. Internet or Intranet
- e. E-mail and Enterprise Instant Messaging (EIM)
- f. Voice Mail
- g. Cell phones (including camera phones and smart phones with data communications and databases)
- h. Pagers
- i. Media including disk drives, diskette drives, optical disks (CD), tape drives, and USB drives (flash drives)
- j. Servers
- k. Printers

#### Unacceptable uses include, but are not limited to the following:

- a. Any use which violates local, state, or federal laws;
  - b. Any use for commercial purposes, product advertisements, or "for-profit" personal activity;
  - c. Any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
  - d. Any use for promotion of political or religious positions or causes;
  - e. Any use in relation to copyright infringement.
  - f. Any use in relation to participating in chain letters or unauthorized chat programs, or forwarding or responding to SPAM;
  - g. Any use for promoting the misuse of weapons or the use of devices associated with terrorist activities;
  - h. Any use related to pyramid selling schemes, multi-marketing schemes, or fundraising for any purpose unless agency sanctioned;
  - i. Any use for dispersing data to customers or clients without authorization;
  - j. Any use in relation to placing wagers or bets;
  - k. Any use that could be reasonably considered as disruptive to another's work;
1. Employees will not waste IT resources by intentionally doing one or more of the following:
- a. Placing a program in an endless loop;

# Appendix A: Technology Usage Practices

## Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 07/01/2015

Page 12 of 14

- b. Printing unnecessary amounts of paper;
  - c. Disrupting the use or performance of State-provided IT resources or any other computer system or network; or
  - d. Storing unauthorized information or software on State-provided IT resources.
- 2. Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:
  - a. Accessing or attempting to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or bypassing State security and access control systems;
  - b. Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;
  - c. Violating the privacy of individual users by reading e-mail or private communications without legal authority, or authorization based upon documented just cause;
  - d. Misrepresenting oneself or the State of West Virginia;
  - e. Making statements about warranty, express or implied, unless it is a part of normal job duties;
  - f. Conducting any form of network monitoring, such as port scanning or packet filtering unless expressly authorized by the WVOT; or
  - g. Transmitting through the Internet confidential data to include without limitation, credit card numbers, telephone calling cards numbers, logon passwords, and other parameters that can be used to access data without the use of encryption technology approved by the WVOT
- 3. Employees will not commit security violations related to e-mail activity. This includes doing one or more of the following:
  - a. Sending unsolicited commercial e-mail messages, including the distribution of "junk mail" or other advertising material to individuals who did not specifically request such material;
  - b. Unauthorized use for forging of e-mail header information;
  - c. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies;
  - d. Posting messages to large numbers of users (over 50) without authorization; or
  - e. Posting from an agency e-mail address to newsgroups, blogs, or other locations without a disclaimer stating that the opinions expressed are strictly their own and not those of the State or the agency, unless posting is in the fulfillment of business duties.

# Appendix A: Technology Usage Practices

## Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001

Issue Date: 01/18/2007

Revised: 07/01/2015

Page 13 of 14

---

### Employee Responsibilities

Employees should conduct themselves as representatives of the State, and are responsible for becoming familiar with and abiding by all information security policies and guidelines.

1. Employees will only access files, data, and protected records if:
  - a. The employee owns the information;
  - b. The employee is authorized to receive the information; or
  - c. The information is publicly available.
2. Employees are prohibited from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, bandwidth, disk space, printer paper, or other IT resources.
3. Employees are prohibited from transmitting personal information about themselves or someone else without proper authorization while using State-provided IT resources.
4. Employees must adhere to copyright law regarding the use of software, print or electronic information, and attributions of authorship. In certain instances, legal counsel can determine permissible uses.



## Appendix B: Policy Understanding and Acknowledgment

### Policy: Information Security

State of West Virginia Office of Technology

Policy No: WVOT-PO1001 Issue Date: 01/18/2007 Revised: 07/01/2015 Page 14 of 14

---

### INFORMATION TECHNOLOGY POLICIES ACKNOWLEDGMENT

From West Virginia Office of Technology  
Office of Information Security and Controls

I have read, understand, and agree to abide by the following West Virginia Office of Technology Information Technology Policies:

- Information Security Policy (WVOT-PO1001)
- Acceptable/Unacceptable Use of State-Provided Technology (WVOT-PO1001, Appendix A)

I understand and agree that if I violate any of the provisions of any of these policies I may be subject to disciplinary action up to and including termination.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Signature Supervisor

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name of Supervisor

**§6-2-1. When official bonds to be given.**

Any person appointed or elected to any office or position in this state who is required by any statute to enter into or give bond, unless otherwise provided, shall give his official bond within sixty days after he has been appointed or duly declared elected; but if at the time of his appointment or election he shall be absent from the state, circuit, county or district for which he is appointed or chosen, he shall give such bond within sixty days after notice of his appointment or election. If no term of the court or other tribunal authorized to take and approve such bond shall be held within sixty days after the appointment or declaration of the election of an officer required by law to give bond and qualify before such court or tribunal, or after the person, if absent from the state, county or district, is notified of his appointment or election, he shall give bond at the first term of such court or other tribunal next thereafter held: *Provided*, That the state executive officers shall qualify on or before the first Monday after the second Wednesday of January next after their election: *Provided further*, That any person appointed or elected to fill a vacancy in any office shall give such bond within ten days after notice of such appointment or election, if the court or other tribunal authorized to take and approve such bond shall sit within said period; otherwise, at the first sitting of such court or other tribunal after notice of such appointment or election. No person shall enter into or discharge any of the duties of his office until he shall have given the bond required of him by law.

*Note: WV Code updated with legislation passed through the [2016 Regular Session](#)*

*The West Virginia Code Online is an unofficial copy of the annotated WV Code, provided as a convenience. It has NOT been edited for publication, and is not in any way official or authoritative.*

**§6-2-6. Bonds of certain state officers.**

The following officers shall give bonds to be approved by the governor, in the penalties hereinafter named: Secretary of state, twenty-five thousand dollars; auditor, fifty thousand dollars; treasurer, five hundred thousand dollars; state superintendent of free schools, three thousand dollars; and commissioner of agriculture, five thousand dollars.

*Note: WV Code updated with legislation passed through the [2016 Regular Session](#)*

*The West Virginia Code Online is an unofficial copy of the annotated WV Code, provided as a convenience. It has NOT been edited for publication, and is not in any way official or authoritative.*



**§6-2-2. How bonds made payable and proved; sureties.**

Every official bond, and every bond required by law to be taken or approved by, or given before, any court, board or officer, shall, unless otherwise provided, be made payable to the state of West Virginia, and shall be signed by one or more sureties deemed sufficient by such court, board or officer, and be proved or acknowledged before, or approved by, such court, board or officer.

*Note: WV Code updated with legislation passed through the [2016 Regular Session](#)*

*The West Virginia Code Online is an unofficial copy of the annotated WV Code, provided as a convenience. It has NOT been edited for publication, and is not in any way official or authoritative.*